２０１７年度 暗号技術検討会 議事概要

1. 日時

平成 30 年 3 月 29 日（木）15:00～17:00

2. 場所

経済産業省本館２階西３共用会議室

3. 出席者（敬称略）

構成員：松本勉（座長）、上原哲太郎、宇根正志、太田和夫、本間尚文、
松井充、松浦幹太、松本泰、向山友也、渡邊創

オブザーバ：内田稔（山本雅亮代理）、岡田崇志（小川久仁子代理）、種田英明、
小高久義、寺田麻倫（阿部知明代理）、小野田和靖（村松秀樹代理）、
本原拓也（小川秀俊代理）、西城泰裕（溝口浩和代理）、
三島崇（森田健太郎代理）、今泉隆文（二宮勉代理）、
吉澤哲太郎（佐野美波代理）、宮崎哲弥、江口純一、大澤昭彦、和田雅昭

事務局：（総務省）澤田稔一、福島千枝、上東孝旭、守屋潤一
（経済産業省）伊東寛、稲垣良一、森川淳
（国立研究開発法人情報通信研究機構（NICT））盛合志帆
（独立行政法人情報処理推進機構（IPA））神田雅透

4. 議事

（１） 文章番号体系について
（２） 2017 年度 暗号技術評価委員会 活動報告について
（３） 2017 年度 暗号技術活用委員会 活動報告について
（４） CRYPTREC 暗号リストの改定について
（５） 2017 年度 暗号技術検討会 報告書（案）について
（６） その他

5. 配付資料

資料１	議事次第・配付資料一覧
資料２	2017 年度 暗号技術検討会 構成員等名簿
資料３	CRYPTREC 文書に対する文書番号の付番方法について
資料４	2017 年度 暗号技術評価委員会 活動報告
資料４別添１	768 ビット素数位数の有限体上の離散対数問題の状況と DSA, DH の今後のパラメータ選択について
資料４別添２	2017 年度　暗号技術調査 WG（暗号解析評価）活動報告
資料４別添３	「暗号技術ガイドライン(SHA-1)」改訂案

資料５	2017 年度 暗号技術活用委員会 活動報告
資料５別添１	「SSL/TLS 暗号設定ガイドライン」改訂案
資料５別添２	「SSL/TLS 暗号設定ガイドライン」改訂案（詳細）
資料６	CRYPTREC 暗号リストの改定について
資料６別添１	3-key Triple DES 及び 64 ビットブロック暗号の今後の利用について
資料６別添２	ChaCha20-Poly1305 の CRYPTREC 暗号リスト追加について
資料６別添３	CRYPTREC 暗号リスト改定案
資料６別添４	CRYPTREC 暗号リスト
資料７	2017 年度 暗号技術検討会報告書（案）

6. 議事概要

6.1. 開会

暗号技術検討会事務局から開会の宣言があり、総務省の澤田審議官から開会の挨拶が行われた。その後、暗号技術検討会事務局より、今井構成員、岡本構成員、近澤構成員、及び手塚構成員が欠席である旨の連絡がなされた。

6.2. 議事

（１） 文章番号体系について

資料３に沿って、暗号技術検討会事務局より説明が行われた。主な質疑は以下のとおり。

宇根構成員：資料 3 に「CRYPTREC ホームページのリニューアルに合わせて反映」とあるが、具体的にいつ頃なのか。

事務局　　：できるだけ上期の早い時期を考えているが、リニューアル作業をこれから始めるので早くても夏頃。

太田構成員：一つの文書に二つの文書番号が付与されることはあり得るのか。

事務局　　：基本的に文書番号が二つ付与されることはないという認識。リビジョンがあるものは R を付けて区別するし、同一のドキュメントであるもののパートで分かれている文書については、各委員会にて管理情報を工夫することで付番する予定。

松本座長　：整理は大変だったと思うが、作業いただき感謝。今後は確認も必要となるがよろしくお願いしたい。

（２） 2017 年度 暗号技術評価委員会 活動報告について

資料４及び別添に沿って、暗号技術評価委員会事務局より説明が行われ、活動報告は原案のとおり承認された。主な質疑は以下のとおり。

松本座長　：今後の予定に素因数分解の困難性に関するグラフのリバイスがあげられているが、離散対数計算についてもリバイスの対象なのか。

事務局　　：素因数分解について大幅な見直しを予定しているが、楕円曲線（離散対数計算）についても、例えば、256 ビットの指標の追加の指摘は暗号技術評価委員会でも頂いているので、その部分の見直しについては検討したい。

松本座長　：楕円曲線は 192 ビットまでしか明示されていないが、実際には、もっと長いものまで使われている。利用する側にとって有益な情報が提供されているのが望ましい。

松井構成員：このグラフは非常に有用であり、一般の方に説明するときに非常に説明し易い。今回も更新いただき感謝。説得力を持って専門外の方に説明することができる。

事務局　　：現在は 2035 年までしか横軸がないが、もう少し先を見据えたグラフがないかという声や、このグラフに載っていないパラメータについても欲しいという声、また、量子コンピュータが実現したときにどうなるかという話も頂いているので、来年度から大きな見直しをしていきたいと考えている。

（3） 2017 年度 暗号技術活用委員会 活動報告について

資料 5 及び別添に沿って、暗号技術活用委員会事務局より説明が行われ、活動報告は原案のとおり承認された。主な質疑は以下のとおり。

宇根構成員：SSL/TLS 暗号設定ガイドラインは 5 月を公開の目安としているが、TLS 1.3 がリリースされそうな時期と競合している。TLS 1.3 が先にリリースされた場合、TLS 1.3 をガイドラインに反映したほうが良いという意見も出るのではないか。

事務局　　：TLS 1.3 に関しては、RFC になっていないバージョンで実装が進んでいること自体は事実だが、今回、特に、高セキュリティ型のところでは、実装物が無いということで、ガイドラインの中身そのものには TLS 1.3 を含めない整理としている。しかし、情報としては TLS 1.3 を含めようということでセクションを追加している。現状はドラフトだが、RFC が発行されたら RFC の番号を入れるし、間に合わなければ「何月時点で RFC の Editor Queue に入ってる」と説明した上で、その後、実際に発行されたタイミングで改定することも考えている。ガイドラインの中身そのものに TLS 1.3 の利用や選択を含めることに関しては、次回のメジャーアップデートの時に考えていくことだが、比較的早いタイミングでの検討

が必要と思っている。

宇根構成員：鍵管理に関する運用ガイドラインについて、調査対象を拝見すると電子証明書の取扱いに関するドキュメントがあまり入っていないと思う。サーバ証明書やルート証明書といった証明書の取扱いは、このガイドラインの中でどのように取り扱おうとしているのか。

事務局　　：調査対象として挙げたのは、まだ、電子証明書やルート証明書などの個別のアプリケーションに落ちていない段階の、一般的な鍵管理に関する文献を集めてきて調べた。宇根構成員がおっしゃったものよりも汎用的なものを想定している。個々の電子署名等ついては、もう一段、次のレイヤーとして考えていくガイドラインと思う。

宇根構成員：来年度の検討の中で考えていくということか。

事務局　　：実際には、鍵管理のガイドラインができた後、第二弾、第三弾として整備していくガイドラインであると考えている。

松本座長　：公開鍵証明書については、鍵管理ガイドラインに含まれてるという理解でよいか。

事務局　　：広い意味では含まれている。

（4） CRYPTREC 暗号リストの改定について

資料 6 及び別添に沿って、暗号技術検討会事務局より説明を行った後、審議が行われた。64 ビットブロック暗号の注釈変更については、事務局案の記載を修正することで承認された。3-key Triple DES の注釈削除及び「電子政府推奨暗号リスト」から「運用監視暗号リスト」への変更、MISTY1 のフルラウンド攻撃への対応及び ChaCha20-Poly1305 の「推奨候補暗号リスト」への追加については、原案のとおり承認された。技術分類「認証暗号」の新設及び注釈の追加については、認証暗号の説明への注釈は不要とした上で承認された。主な質疑は以下のとおり。

（64 ビットブロック暗号の注釈変更について）

上原構成員：内容自体はこれで良いが、「最大 2^{20} ブロックまで」「最大 2^{21} ブロックまで」は、「最大」と「まで」が同じ意味であるから、「最大 2^{20} ブロック」あるいは「2^{20} ブロックまで」とした方がシンプルで良いのではと思う。

松本座長　：冗長という指摘だが、「最大」を取るということでよいか。

事務局　　：いずれの表現が皆様にとって見やすいか。

松浦委員　：日本語らしくするなら、「最大でも」で問題設定し、それに対する回答として「2^{20} ブロックまで」という方法もあるが、どちらでも良い。

松本座長　：類似の表現があるのはどこか。注 12 に「ハッシュ長は 256 ビット以上とすること。」という表現がある。

事務局　　：注 12 に合わせると、これまでのリストと整合が取れると思う。
松本座長　：では、「2^{20}ブロックまで」「2^{21}ブロックまで」と修正いただきたい。

（ChaCha20-Poly1305 の推奨候補暗号リストの追加について）
本間構成員：推奨候補暗号リストへの追加に異論はないが、（注＊）の「CRYPTREC 暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。」が、電子政府推奨暗号リストにも運用監視暗号リストにも含まれていることで混乱を招かないか。つまり、運用監視暗号リストの暗号を組み合わせた認証暗号がどこに入るのか、という混乱が生じないか。
松本座長　：推奨候補暗号リストに ChaCha20-Poly1305 が入ること、そこで「認証暗号」及び「認証付き秘匿モード」に（注＊）が入ること自体は問題ないか。
本間構成員：問題ない。
松本座長　：では、電子政府推奨暗号リストに同じ注釈が入ることは大丈夫か。質問の趣旨は、変なものが含まれてしまわないか、ということか。
本間構成員：然り。組み合わせたものが推奨暗号なのか候補暗号なのか監視対象暗号なのか。
松井構成員：読み方としては、電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リストそれぞれが完結した暗号リストであるという理解ではないか。
本間構成員：ここでいう「CRYPTREC 暗号リスト掲載のブロック暗号」というのは、それぞれ電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リストであって、推奨候補暗号リスト、監視暗号リストについては、該当がないことをもって大丈夫、ということになるのではないか。
太田構成員：そもそも、「認証暗号」のところに（注＊）を加えた趣旨は。
事務局　　：前提として、脚注２に「暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。」とあり、特にどのリストというのは関係なく、組み合わせたものという表現がある。今回、「認証暗号」を新しく技術分類に追加するときに、その技術分類に対する注釈として入れたものだが、「認証暗号」という機能を使いたいという利用者がいたときに今回追加された ChaCha20-Poly1305 だけを「認証暗号」と思ってしまうかもしれないので、これだけが認証暗号ということではなく、例えば、「ブロック暗号」と「認証付き秘匿モード」を組み合わせても「認証暗号」を実現できることを気付いてもらうことが趣旨。その注釈が推奨候補暗号

リストだけにつくのではなく、技術分類に対する注釈なので、多少の重複感はあるが三つのリストそれぞれに付与している。

太田構成員：今ある脚注２の「メッセージ認証コード、エンティティ認証」の間に、「認証暗号」を追加するのでは不十分か。「認証暗号」は、暗号技術の分類に入れるのだから、同じ階層で並んでいるメッセージ認証コードやエンティティ認証とともに、脚注２に追加すればよいのではないか。

事務局　　：「認証暗号」としてもう少し広いものが今のリストに入っていれば良いのだが、現状１つだけが該当していて、ChaCha20-Poly1305 という完全に dedicated な、アルゴリズムまで指定されているもの１つしかない。将来的には、そのような結論で良いかもしれないが、「ブロック暗号」というブラックボックスでなく、アルゴリズムまで指定されてしまっているので、現時点では難しいと思量。

太田構成員：「認証暗号」に脚注を付与した方が良いということか。

松本座長　：電子政府推奨暗号リストの説明の「暗号技術」に脚注２が付いており、推奨候補リストの説明の「暗号技術」にも同じ文言の脚注３が付いている。それから、運用監視暗号リストの「暗号技術」にも同じ文言の脚注４が付いている。ここでの話は、暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているけれども、その場合は CRYPTREC 暗号リストに掲載された暗号で考えることを言っている。それと、「認証暗号」として、「認証付き秘匿モード」と「ブロック暗号」を併せて使うという話は異質なものだと思う。そうすると、「認証暗号」のカテゴリに、注釈を付与しなくても同じではないか。

上原構成員：私は今の場所で良いと思う。電子政府推奨暗号リスト表中の（注＊）はよいと思うが、推奨候補暗号リストと運用監視暗号リストについては、該当する「認証付き秘匿モード」が無いので表中に（注＊）は不要と思う。組み合わせて「認証暗号」ができると言っているが、そもそも「認証付き秘匿モード」に該当する暗号がないので、「認証暗号」として使えるものは存在しえないと思った。電子政府推奨暗号リストは、認証付き秘匿モードとして CCM と GCM があるので（注＊）の意味がある。

本間構成員：CCM や GCM は、各リストを跨いで使うものではないか。

上原構成員：三つのリスト独立にかかるものではなくて、各リスト間のカテゴリをまたいでもいいよという整理なのでは、わかりづらいが。

松本座長　：「認証付き秘匿モード」にだけ注釈を付ければ良いのではないか。

上原構成員：推奨候補暗号リストの「認証付き秘匿モード」に（注＊）があって、「認証暗号」にも同じ（注＊）があるので、後者を削除することで明確になら

ないか。

松本座長　：技術分類の「認証暗号」の（注＊）を削除することで、すっきりしないか。「認証付き秘匿モード」にだけ（注＊）を付与すると、あまり意味がないだろうか。

事務局　　：座長がおっしゃったとおりにするのであれば、推奨候補暗号リストの注釈は、認証暗号として ChaCha20-Poly1305 があるので、「認証付き秘匿モードと組み合わせても」という記載となっている。これについて「も」を取って、「組み合わせて」としたい。

松本座長　：「も」は取った方がよい。その上で「認証暗号」に（注＊）を付けないこととしたい。他に意見はないか。

本間構成員：運用監視暗号リストにも注釈は付けるのか。

松本座長　：技術分類に付与されている注釈は、注釈含めて三つのリストで固定というポリシーで作られている。

本間構成員：承知した。

松本座長　：では、三つのリストとも、「認証付き秘匿モード」に付与する注釈は、「組み合わせて」に統一し、技術分類の「認証暗号」への注釈は付与しないこととしたい。

（議題以外の質疑応答）

太田構成員：案が取れた後の、CRYPTREC 暗号リストの日付は。

松本座長　：平成 25 年に公表されたものが、変更されてきたという整理。これは文書番号の整理で言うとどうなるか。

事務局　　：今回の改定だと 2012R4 となる。

松本座長　：文書番号はこの文面にも付けるべき。

事務局　　：右肩に付けることを想定している。

松本座長　：平成 25 年にはなっているが、本当の改定日は本日になる。いつかは全面改定と思う。

上原構成員：CRYPTREC 暗号リストは、平成 25 年 3 月 1 日に策定したときに 10 年間は同じリストを使用するという方針を定めた。基本的には変わらないものだが、安全性評価等の理由で小改定が行われてきた。大改定のときに前回のような大きなプロセスを経て、この日付も変わるという認識。

（５） 2017 年度 暗号技術検討会 報告書（案）について

資料 7 に沿って、暗号技術検討会事務局より説明が行われた。質疑応答はなく、今後の進め方について承認された。

（6） その他

構成員より以下の意見が表明された。

松本座長　：年一回で非常に効率良く開催できるようになったと思う。2つの委員会の下に WG を作り活動している。事務局の方々も含めて常に努力をされているが、活動が更に認知されるようにしたい。当たり前になってきてしまっているというか、世の中は、放っておけば CRYPTREC が勝手に上手くやってくれるのではないかと期待している。予算や人的な面で努力をして、なんとか回っているというのが実情。この活動が続いていくような仕掛けを、総務省及び経産省、関係各位にも検討いただきたい。

松本構成員：CRYPTREC では、元々、電子政府と言っているが、以前は電子政府と民間の情報システムはイコールだったが、今は暗号の使われている状況に変化がある。自動車や産業系の機器にも組み込まれ始め、電子政府での使われ方と、産業での使われ方が食い違ってきている。特に、新しいイノベーションが起きている業界で暗号技術の利用が進んでいて、典型的には仮想通貨や自動車がある。今、鍵管理が注目されている業界は、仮想通貨業界。暗号の鍵が 580 億円という資産と結びついた。もう1つは自動車業界で、2020 年に販売される自動車から各自動車の ECU に鍵が格納され、とんでもない数の鍵を管理する必要が生じる。ちょうど IoT 機器でパスワード問題とかあるが、人口より多い IoT 機器をパスワードで管理すること自体がナンセンス。そういうことを含めて、暗号の使われ方が変化している。変化に伴って、鍵管理だけではなく、アルゴリズムの考え方やライフサイクルの考え方が変わりつつある。電子政府だけ見ていても世の中の要望に応えられないと思う。電子政府に注力してやるのか、産業競争力の観点から見ていくのか、考えていく必要があると思う。

松本座長　：二年ぐらい前から CRYPTREC のミッションを、暗号リストだけではなく、もう少し広く取り扱っていくこととなったので、御指摘いただいた点は今の枠組みでもできると思う。どうインプリメントしていくかまでは具体化できていないが、重要な指摘だと思う。

6.3. 閉会

経済産業省の伊東審議官から閉会の挨拶が行われた。

また、暗号技術検討会事務局から次回の暗号技術検討会は来年3月頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

以上